

Testing GNSS Receivers Robustness Against Spoofing Attempts

L. Perdue¹, G. Boime², H. Sasaki¹, E. Sicsik-Paré²

¹ Spectracom Corp., 1565 Jefferson Road, Rochester 14623 NY, USA,
lisa.perdue@spectracom.rolia.com
hiro.sasaki@spectracom.rolia.com

² Spectracom SAS, 3 avenue du Canada 91974 Les Ulis FRANCE,
gilles.boime@spectracom.rolia.com
emmanuel.sicsik-pare@spectracom.rolia.com

Abstract:

Spoofing as it applies to GNSS/GPS is an attempt to deceive the GNSS/GPS receiver by broadcasting signals that the receiver will use instead of the live sky signals. A test system for spoofing allows testing the three major factors to consider in a spoofing attack, time synchronization to the signals to be spoofed, power level of the spoofing signal compared to the live sky signals, and accuracy of the position obtained by the spoofing signal to that of the actual position of the device being spoofed.

Receivers can provide some indications that something out of the ordinary is happening during a spoofing attack. But if the system the receiver is integrated into does not monitor or attempt to use these indications, it is difficult to identify a spoofing attack. Understanding how a receiver will respond in a spoofing attack is the key to detecting spoofing. For example, using multiple GNSS systems will prevent a spoofing attack consisting of only GPS. This is only true if the receiver is set up to monitor this type of information.

The spoofing test system allows full control over key parameters in a completely closed system that will not interfere with actual GNSS signals. Each of these variables is described in detail and a sample of three popular, widely-used GNSS receivers test presented. Test results include variations of time, power, and position. Tests are performed using GPS only and also a combination of GPS and GLONASS systems to understand if multi-GNSS is an effective method to overcome spoofing attacks. Using a spoofing test system will allow a user to better understand the GNSS receiver behavior and harden the system against spoofing attacks.

Key words: GNSS, Positioning, Spoofing, Hardening, Simulation.

1. Introduction

Spoofing as it applies to GNSS/GPS is an attempt to deceive the GNSS/GPS receiver by broadcasting signals that the receiver will use instead of the live sky signals. Spoofing is different than jamming. Jamming is easier for a receiver to detect, and while it can disrupt the receiver, it cannot re-locate it. A spoofing system can be used as an attack on systems that use GNSS for precise timing or navigation. A spoofing system can also be used for defensive research. Research ongoing in the defense area on spoofing can be used to control an unmanned autonomous vehicle and re-direct it. A spoofing test system can be used to understand how the receiver reacts in a spoofing situation and monitor and react to prevent the spoofing from occurring. This paper

describes the spoofing test system and how it is used to test receivers. Understanding the behavior of the receiver when faced with a spoofing attack is key to hardening the receiver against spoofing attacks.

2. Spoofing Test System

A spoofing test system can have two different configurations. The first configuration is a live sky antenna used with one simulator and one synchronization system. The simulator is used to spoofing the live sky signals in a controlled environment but this test system gets very complicated quickly. It is hard to determine power levels and difficult to track a moving vehicle. The second configuration is a full laboratory test system and consists of two simulators and one synchronization system. One simulator acts as the live sky signal and

the other as the spoofer. It provides full control over time synchronization, power levels, and both positions. Using two Spectracom GSG units and a Spectracom SecureSync is the preferred method to understand the receiver in order to harden against spoofing attacks.

The test system used for the testing in this paper consists of two Spectracom GSG simulators, one Spectracom SecureSync, an RF switch, and an RF combiner. A PC is used to control the individual units, the RF switch and to monitor the receiver under test. Figure 1 illustrates this test system.

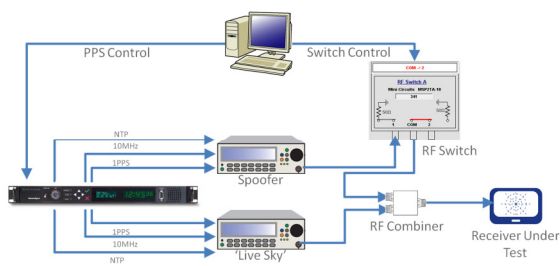


Fig. 1. Spoofing test system.

3. Parameters

There are several parameters that can be varied to help understand how vulnerable a specific receiver is to the spoofing threat. Each of these parameters can be varied independently of the other parameters allowing design of a comprehensive test plan. These parameters are Time, Position, and Power level. Figure 2 shows these parameters.

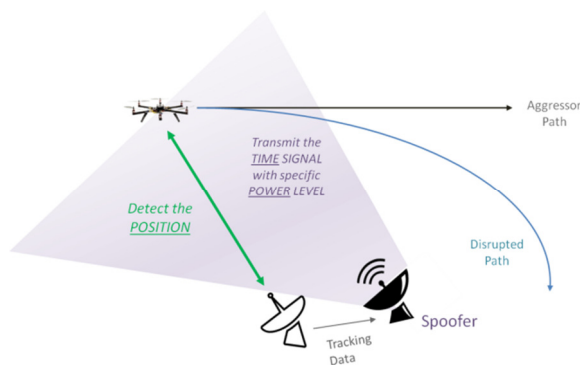


Fig. 2 Important Parameters.

3.1 Time

The timing accuracy of the spoofing signals to the live signals. Utilizing separate outputs from the SecureSync clock system, the PPS offset can be varied. These PPS signals are used as triggers to the GSG Simulator units and therefore cause an offset in time between the

two RF signals. This offset is controllable to the nanosecond level.

Another time to consider in the test design is the capture time. This is how long the spoofing signal is applied before attempting to re-direct the receiver. Figure 3 shows the interface in the SecureSync for applying the offset.

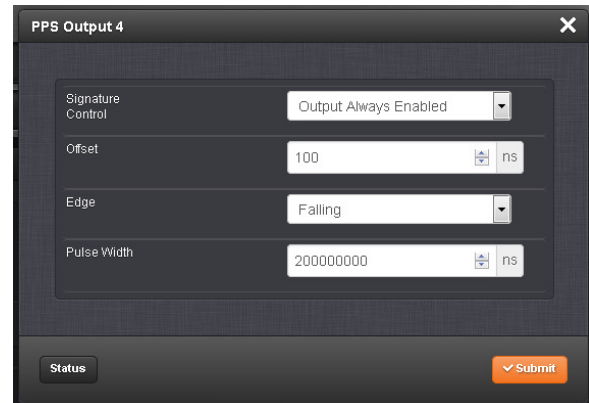


Fig. 3 SecureSync PPS Offset Interface.

3.2 Position

The position provided by the spoofer must be accurate to that of the receiver to be spoofed. Exactly how close the spoofer must be to the receiver position is a variable parameter and can be different based on receiver settings, receiver manufacturer, and initial conditions (moving vs. stationary). Using two simulators allows full control of the two positions so many different test cases can be designed and executed to understand the receiver limitations. The more accurate the spoofer must be to successfully take control of the receiver, the more difficult it will be for an attacker to spoof the receiver. Figure 4 shows an example of the two different positions with a 500m offset.



Fig. 4 500m Position Offset.

3.3 Power

The spoofing signal should be greater than the live signal in order to capture the receiver. The

spoofing test system allows full control of the power levels to determine how much greater the power should be. Too much power will jam the receiver. The test system allows testing of the receiver to try and determine if there are any indicators given by the receiver when a signal only a few dB higher than the transmitted signal is received.

4. Test Cases

Several test cases were designed to observe the effects of varying the critical parameters and attempting to spoof the receiver.

Four TIME offset test cases were created. For these cases the position offset was 0 meters and the power level of the spoofer was 2dB higher than the live sky simulator. Offsets of 1 nanosecond, 100 nanoseconds, 500 nanoseconds, and 1.5 microseconds were tested.

Three POSITION offset test cases were created. For these test cases the time offset was set to 1 nanosecond and the power level of the spoofer was 2dB higher than the live sky simulator. Offsets of 50 meters, 250 meters, and 500 meters were tested.

Three POWER offset test cases were created. For these test cases the time offset was set to 1 nanosecond and the position offset is set to 0 meters. Offsets of 2dB, 1dB, and 0dB were tested.

Finally there was a test created for multi-GNSS. In this case the live sky simulator was set to simulate GPS and GLONASS. The spoofer was set to GPS-only. The position offset was set to 0 meters, the time offset was set to 1 nanosecond, and the power level of the spoofer was 2dB higher than the live sky simulator.

Figure 5 summarizes the test cases.

TIME Offsets	POSITION Offsets	POWER LEVEL Offsets	Multi-GNSS
<ul style="list-style-type: none"> • 1ns • 100ns • 500ns • 1.5usec 	<ul style="list-style-type: none"> • 50m • 250m • 500m 	<ul style="list-style-type: none"> • 2dB • 1dB • 0dB 	<ul style="list-style-type: none"> • Live Sky • Multi-GNSS • Spoofer • GPS-only
Position Offset 0m Power +2dB	Time Offset 1ns Power +2dB	Position Offset 0m Time Offset 1ns	Position Offset 0 Time Offset 1ns Power +2dB

Fig. 5 Test Cases.

5. Test Implementation

The test set up was configured to execute the following sequence:

- **T=0 Start Automated Test Scenario**
 - Live Sky Only (static position)
 - Spoofer is not switched in
- **ΔT=3min Enable Spoofer**
 - Combine Live Sky with the Spoofer set to the starting position
 - Spoofer is automatically switched in
- **ΔT=5sec Initiate Spoofer Trajectory**
 - Spoofer position begins to change via GSG Simulator predefined scenario:
 - 90 degree heading; 10m/s speed
 - Allows a 5 second capture time
- **ΔT=30sec and ΔT=60sec Automated Data Measurement**
 - Results from receiver's reported position are logged for analysis

Using this sequence tests can be performed in a repeatable and consistent manner, helping to understand the receiver and how its performance is affected when a spoofing attack is attempted.

6. Test Results

Three receivers were used to perform the test cases.

- Septentrio AsteRx3 OEM Receiver (R1)
- Ublox NEO-M8N (R2)
- Inventek USB-GPS / SiRFstarIII (R3)

It is important to note that receiver should perform a cold start at the beginning of each test sequence to maintain consistent behavior from test to test. Otherwise recently accumulated data and position/time solutions will influence the dynamic response of the navigation solution.

The test results can be analyzed by comparing the logged positions from the receiver at 30 seconds and 60 seconds after the movement has started. The results summary for 2D position is shown in Table 1. Each case is categorized as not spoofed, partially spoofed, or fully spoofed. Not spoofed (No) means the position did not change from the live sky position. Partially spoofed (P) means the position was changed but was not that of the live sky simulator or the spoofer. Fully spoofed (Yes) means the receiver position was that of

the spoofer. N/A indicates mode not available in the receiver.

We can see R1 and R2 receivers are more robust to spoofing signals since they request a lower positioning and time offset error to be captured by the fake signal.

Full test results are given in Appendix A. At 30 seconds the spoofer 2D position is 300 meters away from the live sky position. At 60 seconds, it is 600 meters away. The altitude of live sky and spoofer position remains the same, so any deviation from 0m is due to the spoofing signals.

Tab. 1: Test Results Summary

		R1	R2	R3
POSITION TIME	1ns	Yes	Yes	Yes
	100ns	Yes	Yes	Yes
	500ns	P	P	Yes
	1.5us	No	No	No
POSITION N	50m	Yes	Yes	Yes
	250m	Yes	P	P
	500m	P	P	P
POWER	2dB	Yes	Yes	Yes
	1dB	Yes	Yes	P
	0dB	P	No	P
MULTI-GNSS	Multi-GNSS with GPS Spoof	No	No	N/A

7. Conclusion

The Spoofing Test System allows for better characterization through systematic repeatable tests of receiver performance in the presence of a spoofer. By monitoring the available parameters given by the receiver it may be possible to identify and even overcome a spoofing attack. Monitoring loss of lock, receiver noise, IMU system, and estimated position error are possible parameters to observe but each receiver may report different indications. Receivers may also have different modes of operation to test and observe the results.

Observed results provide insight into how different receivers respond to the same threat. More test cases can be created and performed using the features of the spoofing test system in order to fully characterize a receiver and how it responds to a spoofing attack.

Biographies

Lisa Perdue is an applications engineer at Spectracom and a specialist in GNSS simulation. She has more than 15 years of

navigation and RF systems experience, including 10 years of US Naval Service.

Gilles Boime is Chief Scientist at Spectracom. He has more than 34 years of signal intelligence and GNSS signal management experience. He is leading technology advisory and partnership for Spectracom. He contributes to the early standardization activities for Galileo European GNSS. He holds an engineer graduate from Institut Supérieur d'Electronique de Paris with Telecommunication option.

Hironori Sasaki – Director of Solutions Architecture at Spectracom. Hiro has over 11 years of experience designing, selling and implementing communication systems for Government and Military organizations around the World. Hiro joined Spectracom in 2014 with a focus on leading the organization in expanding the system solutions and program business. Hiro holds a BS in Computer and Systems Engineering from Rensselaer Polytechnic Institute and an MBA from the University of Rochester's NY Simon School of Business.

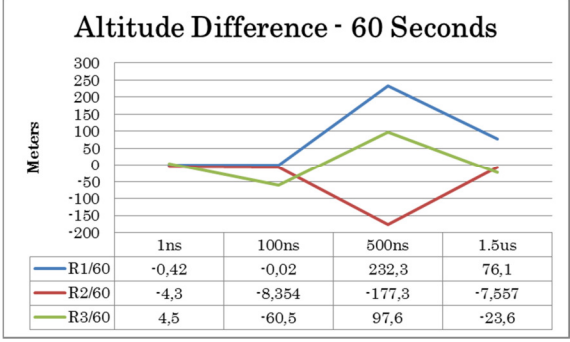
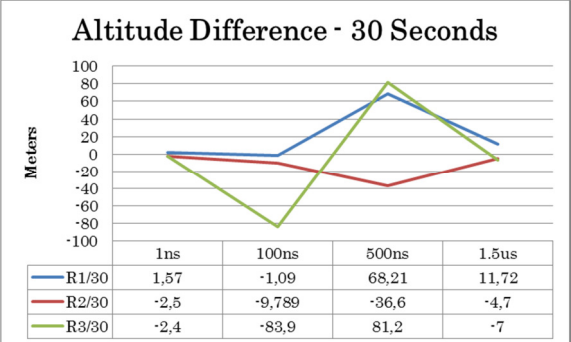
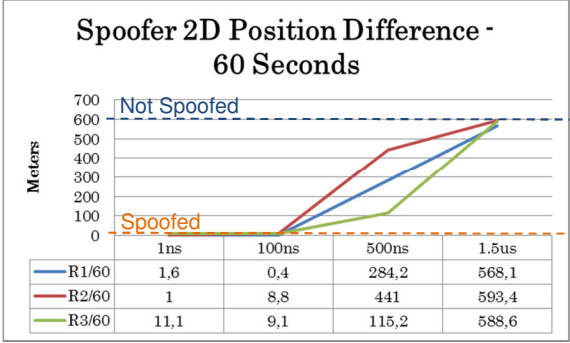
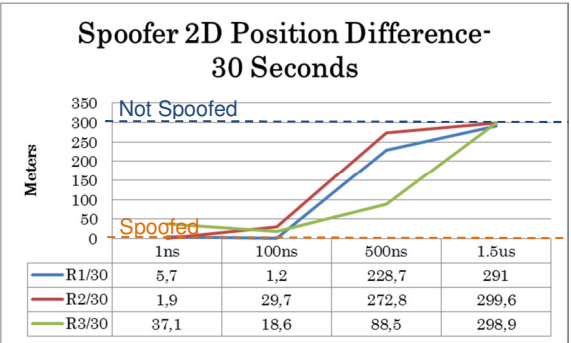
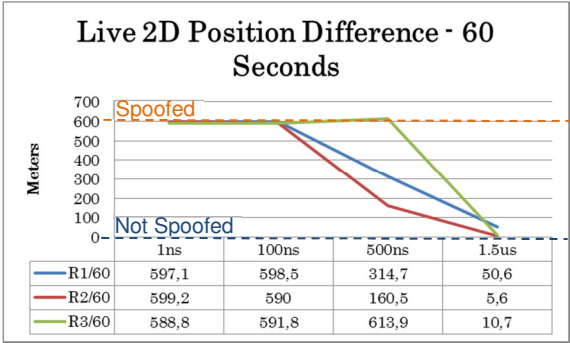
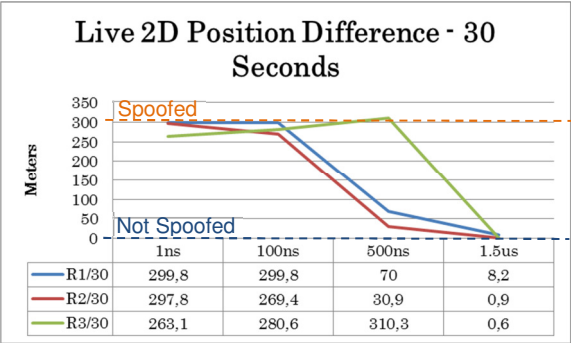
Emmanuel Sicsik-Pare is Strategic Product Manager at Spectracom. Following a first position in radar / optronics program management in French Ministry of Defense, Emmanuel held various positions in Spectracom, focusing on new products and solutions in the Positioning, Navigation and Timing domain. Emmanuel holds a MSc in Telecommunications from Telecom Bretagne.

References

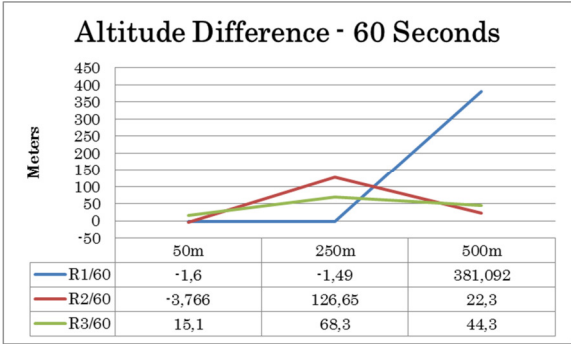
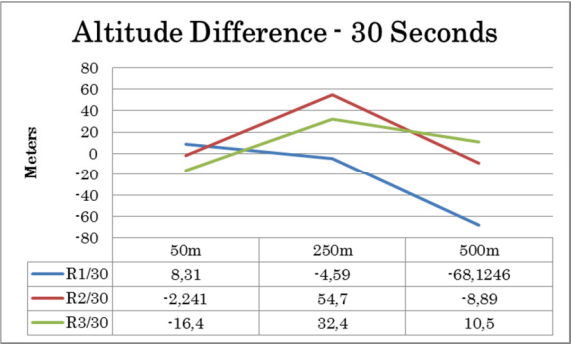
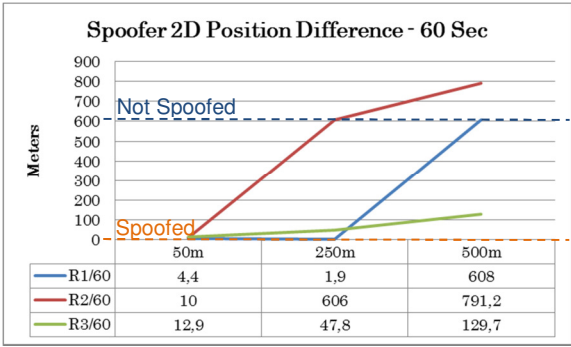
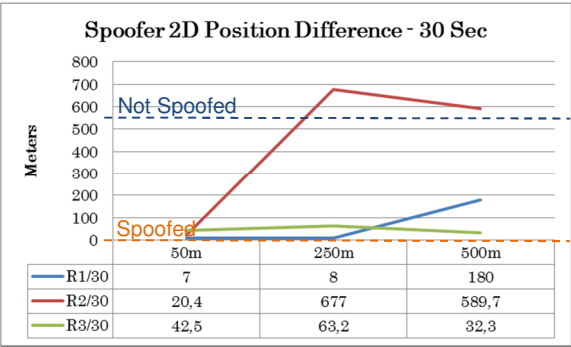
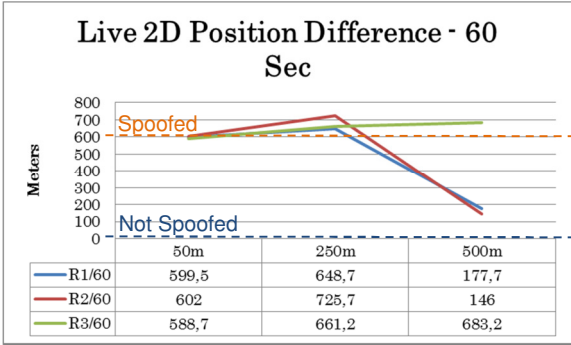
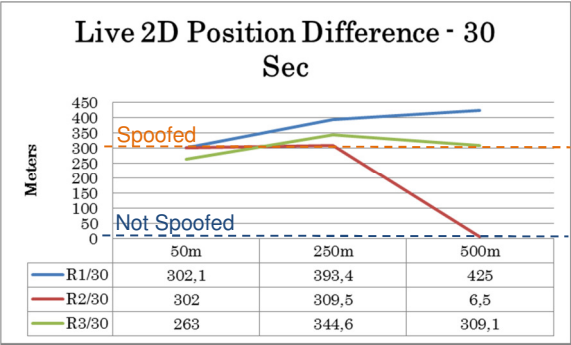
- B. Parkinson, J. Spilker, GPS Theory and Applications, *American Institute of Aeronautics and Astronautics*
- E. Kaplan, C. Hegarty, Understanding GPS: Principles and Applications, *Artech House*
- P. Misra, P. Enge, Global Positioning System: Signals, Measurements and Performance, *Ganga-Jamuna Press*
- F. Dovis, GNSS Interference Threats and Countermeasures, *Artech House*
- T. Humphreys and Allied, Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer, *Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008)*, Savannah, GA, September 2008, pp. 2314-2325
- H. Kuusniemi, Effects of GNSS Jammer and Potential Mitigation Approaches, *UN/Latvia Workshop on the Applications of GNSS 2012*

Annex A: Test Results

Time Offset Results



Position Offset Results



Power Offset Results

